UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

ELIZABETH SINES, ET AL., | **Case No. 3:17-cv-00072-NKM**

Plaintiffs, | **Hon. Norman K. Moon**

v.

JASON KESSLER, ET AL.,

Defendants.

DEFENDANT MICHAEL PEINOVICH'S REPLY MEMORANDUM IN FURTHER SUPPORT OF HIS 1) MOTION TO QUASH PLAINTIFFS' SUBPOENAS TO TWITTER, GODADDY, CLOUDFLARE, AND HATREON, AND 2) MOTION TO REQUIRE PLAINTIFFS' FULL COMPLIANCE WITH FED. R. CIV. P. 45(a)(1)(D)(4) AND (b)(4) OR IN THE ALTERNATIVE TO QUASH

Defendant Michael Peinovich, Pro Se, submits this reply memorandum in further support of his motions 1) to quash plaintiffs' subpoenas to Twitter, Inc., Godaddy.com, LLC, Cloudflare, LLC, and Hatreon, and for a protective order, pursuant to Fed. R. Civ. P. 45, and 2) motion to require plaintiffs' full compliance with Fed. R. Civ. P. 45(a)(1)(D)(4) and (b)(4) or in the alternative to quash. Plaintiffs combined their opposition to Peinovich's motions in a single memorandum; Peinovich, accordingly, combines his reply to plaintiffs' opposition in a single memorandum.

ARGUMENT

An aspect of the current American political and cultural environment that is particularly relevant to Peinovich's motion to quash (or for a protective order) is the growing incidence of doxxing and related types of cyber warfare, such as cyber-vigilantism, hactivism, and cyber-bullying. Doxxing and cyber-vigilantism, as the Court is no doubt aware, involve use of targeted

persons' private and confidential information, such as names (where anonymity is desired), addresses, places of employment, telephone numbers, and personal relationships, to disrupt or cause loss of employment, disrupt or destroy personal relationships, harass through, *e.g.*, sign and internet postings and unwanted telephone calls, and generally incite trepidation in the lives of the targets and those around them. Doxxing and other forms of cyber warfare are favored techniques of AntiFa, which participated alongside other counterprotestors, including many of the plaintiffs, at the events in Charlottesville. *See, e.g.,* https://www.wired.com/2017/03/meet-daryle-lamont-jenkins-insatiable-doxxer-fascists-nazis/. As noted in the article attached above: "In [Daryle Jenkins', AntiFa activist's] utilitarian worldview, all's fair when you're fighting hate. But exposing people's personal information—their addresses, their places of employment, their schools—can cause real-world harm."); *see also*: https://www.infowars.com/new-jersey-homeland-security-officially-lists-antifa-as-a-terrorist-organization/ (AntiFa listed as terrorist organization). The accelerating use of doxing and cyber-vigilante tactics, and specifically its use by the Charlottesville counterprotestors, was noted in a recent article in the New York Times entitled "How 'Doxxing' Became a Mainstream Tool in the Culture Wars": https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html. As this article stated:

> Now the online hunt to reveal extremists has raised concerns about unintended consequences, or even collateral damage. A few individuals have been misidentified in recent weeks, including a professor from Arkansas who was wrongly accused of participating in the neo-Nazi march. And some worry that the stigma of being outed as a political extremist can only reinforce that behavior in people who could still be talked out of it.
>
> * * *
>
> Charlottesville has made doxxing even more commonplace.

> "For a long time it was only a certain quarter of people on the internet who would be willing to do this," Ms. Coleman said. "It was very much hinged on certain geek cultures, but there was an extraordinary quality to the Charlottesville protest. It was such a strong public display I think it just opened the gates."
>
> The right-wing rally ultimately fizzled on Saturday, but counter-protesters were still on the lookout.
>
> "It's important to dox Nazis," said Andrea Grimes, 33, of Alameda, Calif. She held a sign that read: "White people pick one: Be the problem. Be the solution." She said she had "outed" white supremacists to their parents, which she said often worked well to stop bad behavior online.

Instances of doxxing and other cyber-vigilante tactics causing grave harm are legion. In the case of Tony Hovater, for example, Mr. Hovater lost his job and was forced to leave his home. See https://www.cnbc.com/2017/12/08/doxxing-someone-even-if-hes-a-nazi-sympathizer-poses-a-serious-ethical-dilemma.html.

Against this background, plaintiffs' assertion that Peinovich has failed to show a personal right in the information sought by the subpoenas, and therefore lacks standing, is ill-founded. As Peinovich averred in his initial memorandum, he is the host of a podcast on therightstuff.biz that has tens of thousands of weekly listeners and is Peinovich's means of support. The podcast is controversial, as plaintiffs concede. The identities of many of the listeners and supporters of the podcast are at risk of being revealed if Twitter and the other subpoenaed companies comply with plaintiffs' broad document and information requests. If their identities were revealed, these listeners and supporters could be exposed to doxxing and other cyber warfare tactics. They would thereby be harmed, perhaps severely, and Peinovich would likewise be harmed because persons would be apprehensive to stay or become listeners or supporters of his podcast. Indeed, Peinovich has standing not only in his own right but on behalf of his listeners and supporters. *See, e.g., Enterline v. Pocono Medical Center, Inc.,* 751 F. Supp.2d 782, 784-86 (M.D.Pa. 2008)

(newspaper, in opposing subpoena, had standing to invoke First Amendment rights of anonymous commentators on newspaper's website); *McVicker v. King*, 266 F.R.D. 92, 94-97 (W.D. Pa. 2010) (media company, opposing subpoena, had standing to assert anonymous bloggers' rights); *see also Cooksey v. Futrell*, 721 F.3d 226, 235 (4th Cir. 2013) ("In First Amendment cases, the injury-in-fact element [for standing] is commonly satisfied by a sufficient showing of 'self-censorship, which occurs when a claimant is chilled from exercising h[is] right to free expression.'") (internal citation to embedded quotation omitted).

It is no answer to assert, as plaintiffs have done, that such dangers can be obviated by means of the parties' confidentiality agreement. The quantity of information plaintiffs seek by means of the subpoenas is enormous: Plaintiffs seek information that includes but is not limited to personally identifiable information on hundreds of thousands of private citizens who have done nothing more than visit a website. Plaintiffs are seeking personally identifiable information on visitors to dailystormer.com, alright.com and therightstuff.biz for the dates August 1 to August 19, 2017, as well as a multitude of other documents concerning the free speech rally on August 12, any tweets with particular hashtags, and personally identifiable information about any twitter users that tweeted using those hashtags. Plaintiff's motivation to protect this information from hacking, inadvertent disclosure, or even intentional disclosure is dubious, given the plaintiffs' obvious animus toward Peinovich and the other defendants. Moreover, perception in this context is reality: Peinovich's listeners and supporters are highly unlikely to have confidence that their personal identifying information, entrusted to plaintiffs' counsel, will not be inadvertently or intentionally leaked. Merely allowing the subpoenas to proceed will have a chilling effect on the exercise of their First Amendment rights by Peinovich and his listeners and

supporters. Peinovich in fact affirmatively avers under oath that numerous of his listeners and supporters have expressed to him great trepidation about becoming the targets of doxxing and other cyber attacks as a result of the subpoenas to Twitter and the other companies.

Plaintiffs' contention that the harm to Peinovich does not fit into the pigeonholes plaintiffs' claim solely apply is also misbegotten. Harm to Peinovich's vocation and business is manifestly an "undue burden." So too is disclosure to plaintiffs of information having no legitimate bearing on this case. *See Singletary v. Sterling Transport Company*, 289 F.R.D. 237, 241 (E.D. Va. 2012).

The error in plaintiffs' contention that Peinovich has filed his motion to quash in the wrong court is tied to the plaintiffs' improper disregard of Rules 45(a)(1) (D)(4) and (b)(4). Peinovich cannot know with certainty where, when, and from which court plaintiffs filed their subpoenas, except as to Cloudflare, because plaintiffs have concealed this information except as to Cloudflare. For the reasons stated in Peinovich's initial memorandum, such hiding of relevant information contravenes the letter and spirit of Rules 45(a)(1)(D)(4) and (b)(4), whose purpose is to give parties such as Peinovich fair notice so they can oppose the subpoenas before they become a fait accompli. Plaintiffs claim they complied with these rules, but the subpoena information they provided, except as to Cloudflare, lacked information as to the specific address of the party subpoenaed, the date the subpoena was served, and even the court that issued the subpoena.

It is telling in this regard to examine the information that plaintiffs, for whatever reason, provided as to Cloudflare. (See Exhibit 5, document 229, Peinovich's Motion to compel compliance with rule 45) This information shows not only the date of the subpoena and address

of the party subpoenaed, but the court that issued it: this Court. This Court, accordingly, is a "district where compliance is required." *See, e.g., AGV Sports Group, Inc. v. Protus IP Solutions, Inc.*, 2010 WL 1529195 at * 5 (D. Md. Apr. 15, 2010) ("this Court has the authority to quash or modify subpoenas issued from this Court"). If Cloudflare were to disregard the subpoena, it would be violating this Court's order. It appears highly likely that plaintiffs' subpoenas to Twitter, GoDaddy, and Hatreon were also issued from this Court. Plaintiffs' opposition memorandum is equivocal about this, probably deliberately so, but given that plaintiffs treat the Cloudflare subpoena no differently from the other subpoenas in their arguments the inference is strong that all four subpoenas issued from this Court.

Plaintiffs have also accused Peinovich of refusing to confer with them in good faith over discovery disputes prior to seeking a remedy from the Court, but as Exhibit 4 to Peinovich's original motion to compel (document 229) demonstrates it was counsel for plaintiffs Christopher Greene that refused to confer concerning these subpoenas. Peinovich in good faith reached out to Greene to ask about these matters and was at first stonewalled and then later given a dismissive response in which Greene took the extraordinary step of telling Peinovich he would submit documents on his behalf.

CONCLUSION

Plaintiffs hope to use the Court's subpoena power to gather intelligence on individuals they disagree with politically in order to target them for harassment. Not only is the information requested not necessary or relevant to the plaintiffs' case but its release risks harming numerous people, including Peinovich, if granted. It also will injure the privacy rights of potentially

hundreds of thousands of individuals and the reputations of the various companies named above, all of whom would likely suffer reduced subscriber and user counts because the individuals cannot trust that their information will be kept private by these companies. It would further have a chilling effect on free speech generally as individuals who would like to consume or produce politically incorrect, conservative, pro-Trump, pro-white, right wing, or other controversial content would feel they may be subject to doxing, intimidation, and harassment.

For these reasons, Peinovich respectfully requests that the Court quash plaintiffs' subpoenas to Twitter, GoDaddy, Cloudflare, and Hatreon and grant Peinovich's Motion for a Protective Order.

Dated: March 7, 2018

Respectfully submitted,

Michael Peinovich, Pro Se

CERTIFICATE OF SERVICE

On this 7th day of March, 2018, I Michael Peinovich certify that I served electronically or mailed copies of this reply memorandum to:

Christopher Greene <cgreene@kaplanandcompany.com>,

David Campbell <DCampbell@dhgclaw.com>,

Elmer Woodard <isuecrooks@comcast.net>,

James Kolenich <jek318@gmail.com>,

Bryan Jones <bryan@bjoneslegal.com>,

Roberta Kaplan <rkaplan@kaplanandcompany.com>,

Julie Fink <jfink@kaplanandcompany.com>,

Gabrielle Tenzer <gtenzer@kaplanandcompany.com>,

Alan Levince <alevine@cooley.com>,

Karen Dunn <KDunn@bsfllp.com>,

Philip Bowman <pbowman@bsfllp.com>

Michael Peinovich